UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/693,290	10/23/2003	Christopher J. Kaler	13768.302.1.1	4141

47973 7590 09/20/2007

WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER	
FIELDS, COURTNEY D	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
09/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/693,290	KALER ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 July 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27,35-42 and 44-71* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27,35-42 and 44-71* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *05 July 2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 28-34 and 43 have been cancelled.

2. Claims 1-27,35-42, and 44-71 are pending.

Information Disclosure Statement

3. The Information Disclosure Statement respectfully submitted on 05 July 2007 has been considered by the Examiner.

Response to Arguments

4. Applicant's arguments with respect to claims 1-20,22-27,35-40,42, 44-50,52,54-62, and 64-69 have been considered but are moot in view of the new ground(s) of rejection, Maruyama et al. (US Patent No. 6,990,585).

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-20,22-27,35-40,42, 44-50,52,54-62, and 64-69 are rejected under 35 U.S.C. 102(e) as being anticipated by Maruyama et al. (US Patent No. 6,990,585).

Referring to the rejection of claims 1 and 23, Maruyama et al. discloses in a network environment that includes a plurality of computing systems capable of

communicating using electronic messaging, a method for a source computing system constructing an electronic message, the method comprising the following:

an act of designating at least one destination address in the electronic message, the destination address corresponding to one or more recipient computing devices; (See Column 5,lines 33-40)

an act of including a first security token in a header portion of the electronic message, the first security token being at least derived from a first credential of a first credential type; (See Column 6,lines 22-24)

and an act of including a second security token in the header portion of the electronic message, the second security token being at least derived from a second credential of a second credential type (See Column 6,lines 16-19)

Referring to the rejection of claim 2, Maruyama et al. discloses the claimed limitation wherein the first security token is biometric data (See Column 5,lines 13-14)

Referring to the rejection of claim 3, Maruyama et al. discloses the claimed limitation wherein an act of including an encryption manifest in the header portion to thereby designate portions of a body portion of the electronic message that are encrypted (See Column 3,lines 44-46)

Referring to the rejection of claim 4, Maruyama et al. discloses the claimed limitation wherein an act of transmitting the electronic message with the first security token and the second security token in the header portion to the one or more recipient computing devices (See Column 3, lines 46-51)

Referring to the rejection of claim 5, Maruyama et al. discloses the claimed limitation wherein the first security token is the first credential (See Column 6, lines 36-39)

Referring to the rejection of claim 6, Maruyama et al. discloses the claimed limitation wherein the first security token is a first signature that was generated using the first credential (See Column 5, lines 43-49)

Referring to the rejection of claim 7, Maruyama et al. discloses the claimed limitation wherein an act of including the first credential in the electronic message (See Column 6, lines 27-32)

Referring to the rejection of claim 8, Maruyama et al. discloses the claimed limitation wherein the second security token is the second credential (See Column 6, lines 33-35)

Referring to the rejection of claim 9, Maruyama et al. discloses the claimed limitation wherein the second security token is a second signature that was generated using the second credential (See Column 6, lines 47-49)

Referring to the rejection of claim 10, Maruyama et al. discloses the claimed limitation wherein an act of including the second credential in the electronic message (See Column 6, lines 2-6)

Referring to the rejection of claim 11, Maruyama et al. discloses the claimed limitation wherein the at least one destination address corresponds to at least a first and a second recipient computing system, the first computing system using the first credential to identify the source computing system, and the second computing system

using the second credential to identify the source computing system (See Column 7, lines 53-54)

Referring to the rejection of claims 12 and 25, Maruyama et al. discloses the claimed limitation wherein an act of determining that the first recipient computing system uses the first credential to identify the source computing system; (See Column 6,lines 22-24)

and an act of determining that the second recipient computing system uses the second credential to identify the source computing system (See Column 6,lines 16-19)

Referring to the rejection of claim 13, Maruyama et al. discloses the claimed limitation wherein the at least one destination address corresponds to at least a first recipient computing system that uses both of the first credential and the second credential to identify the source computing system (See Column 5,lines 33-40)

Referring to the rejection of claims 14 and 26, Maruyama et al. discloses the claimed limitation wherein an act of determining that the first recipient computing system uses both of the first credential and the second credential to identify the source computing system (See Column 7, lines 53-54)

Referring to the rejection of claim 15, Maruyama et al. discloses the claimed limitation wherein the at least one destination address corresponds to at least a first recipient computing system that uses the first credential and the second credential to identify the source computing system, the electronic message also traversing through an intermediary computing system that uses the second credential to identify the source computing system (See Column 5,lines 33-40)

Referring to the rejection of claims 16 and 27, Maruyama et al. discloses the claimed limitation wherein an act of determining that the first recipient computing system uses the first credential to identify the source computing system; (See Column 6,lines 22-24)

and an act of determining that the intermediary computing system uses the second credential to identify the source computing system (See Column 5,lines 33-40)

Referring to the rejection of claim 17, Maruyama et al. discloses the claimed limitation wherein an act of designating an intermediary address that corresponds to the intermediary computing device (See Column 5,lines 33-40)

Referring to the rejection of claim 18, Maruyama et al. discloses the claimed limitation wherein an act of encoding the first security token;

an act of including, in the header portion, an identification of an encoding format of the first security token; (See Column 4, lines 10-22)

and an act of including, in the header portion, an identification of a type of the security token (See Column 4, lines 23-29)

Referring to the rejection of claim 19, Maruyama et al. discloses the claimed limitation wherein the security token comprises a credential (See Column 6, lines 36-39)

Referring to the rejection of claim 20, Maruyama et al. discloses the claimed limitation wherein the first security token is a signature generated by a user, the method further comprising:

an act of generating a reference indicating where a credential associated with the user may be found; (See Column 6,lines 22-24)

an act of including the reference in the header portion of the electronic message (See Column 4, lines 23-29)

Referring to the rejection of claim 22, Maruyama et al. discloses the claimed limitation wherein the electronic message is a HyperText Transport Protocol (HTTP) message, and wherein the header portion is a header portion of the HTTP message (See Column 8, lines 48-57)

Referring to the rejection of claim 24, Maruyama et al. discloses the claimed limitation wherein the one or more computer-readable media are physical storage media (See Column 4, lines 50-61)

Referring to the rejection of claims 35 and 37, Maruyama et al. discloses a computer program product for use in a network environment that includes a plurality of computing systems capable of communicating using electronic messaging, a method for identifying a source computing system of an electronic message, the computer program product comprising one or more computer-readable media having stored thereon the following:

computer-executable instructions for detecting the receipt of an electronic message; (See Column 5,lines 33-40)

computer-executable instructions for selecting one of a plurality of credentials included in a header portion of the electronic message; (See Column 7, lines 53-54)

and computer-executable instructions for identifying the source computer system using the selected credential (See Column 4, lines 23-29)

Referring to the rejection of claims 36 and 38, Maruyama et al. discloses the claimed limitation wherein the one or more computer-readable media are physical storage media (See Column 4, lines 50-61)

Referring to the rejection of claim 39, Maruyama et al. discloses the claimed limitation wherein the computer-executable instructions for determining how to handle the credential and the electronic message comprise the following:

computer-executable instructions for consulting handling rules of at least one ancestral credential in the logical hierarchical tree; (See Column 5,lines 33-40)

computer-executable instructions for consulting extended handling rules specific to the credential included in the electronic message; (See Column 6,lines 22-24)

and computer-executable instruction for determining handling rules for the credential included in the electronic message by using the handling rules for the at least one ancestral credential as well as the extended handling rules specific to the credential included in the electronic message (See Column 6,lines 16-19)

Referring to the rejection of claim 40, Maruyama et al. discloses the claimed limitation wherein the credential includes biometric data (See Column 5,lines 13-14)

Referring to the rejection of claim 42, Maruyama et al. discloses the claimed limitation wherein the electronic message is a HyperText Transport Protocol (HTTP) message, and wherein the header portion is a header portion of the HTTP message (See Column 8, lines 48-57)

Referring to the rejection of claims 44 and 56, Maruyama et al. discloses in a network environment that includes a plurality of computing systems capable of

communicating using electronic messaging, a method for a source computing system constructing an electronic message, the method comprising the following:

an act of encoding a credential that identifies the source computing device; (See Column 4, lines 10-22)

an act of including the credential in a header portion of an electronic message; (See Column 4, lines 23-29)

and an act of including, in the header portion, information indicative of a type of the credential (See Column 4, lines 23-29)

Referring to the rejection of claim 45, Maruyama et al. discloses the claimed limitation wherein the information indicative of a type of the credential comprises a human-readable expression of the type of the credential (See Column 5, lines 11-19)

Referring to the rejection of claim 46, Maruyama et al. discloses the claimed limitation wherein the information indicative of a type of the credential comprises information that is not a human-readable expression of the type of the credential, but nonetheless is information from which the type of credential may be derived (See Column 6, lines 36-39)

Referring to the rejection of claim 47, Maruyama et al. discloses the claimed limitation wherein an act of including in the header portion, an identification of an encoding format of the credential (See Column 4, lines 10-22)

Referring to the rejection of claim 48, Maruyama et al. discloses the claimed limitation wherein an identification of an encoding format of the credential is not included

in the header portion thereby indicating that a default encoding format has been applied (See Column 4, lines 23-29)

Referring to the rejection of claim 49, Maruyama et al. discloses the claimed limitation an act of including an encryption manifest in the header portion to thereby designate portions of a body portion of the electronic message that are encrypted (See Column 3,lines 44-46)

Referring to the rejection of claim 50, Maruyama et al. discloses the claimed limitation wherein the credential includes biometric data (See Column 5,lines 13-14)

Referring to the rejection of claim 52, Maruyama et al. discloses the claimed limitation wherein the electronic message is a HyperText Transport Protocol (HTTP) message, and wherein the header portion is a header portion of the HTTP message (See Column 8, lines 48-57)

Referring to the rejection of claim 54, Maruyama et al. discloses the claimed limitation wherein the credential is in a binary format, wherein the act of including, in the header portion, an identification of a type of the credential comprises an act of including, in the header portion, an indication that the credential has the binary format (See Column 5,lines 33-40)

Referring to the rejection of claim 55, Maruyama et al. discloses the claimed limitation wherein the credential is in a binary format, wherein the act of including, in the header portion, an identification of a type of the credential comprises an act of including, in the header portion, an indication that the credential has the binary format (See Column 5,lines 33-40)

Referring to the rejection of claim 57, Maruyama et al. discloses wherein the one or more computer-readable media are physical storage media (See Column 4, lines 50-61)

Referring to the rejection of claim 58, Maruyama et al. discloses in a network environment that includes a plurality of computing systems capable of communicating using electronic messaging, a method for a source computing system constructing an electronic message, the method comprising the following:

an act of including an electronic signature in a header portion of an electronic message, the electronic signature generated by a user; (See Column 4, lines 10-22)

an act of generating a reference indicating where a credential associated with the electronic signature may be found; (See Column 4, lines 23-29)

an act of including the reference in the header portion of the electronic message (See Column 4, lines 23-29)

Referring to the rejection of claim 59, Maruyama et al. discloses wherein an act of including an encryption manifest in the header portion to thereby designate portions of a body portion of the electronic message that are encrypted (See Column 3,lines 44-46)

Referring to the rejection of claim 60, Maruyama et al. discloses wherein the reference indicates that the associated credential may be found at a location that is internal to the electronic message (See Column 6, lines 36-39)

Referring to the rejection of claim 61, Maruyama et al. discloses wherein the reference indicates that the associated credential may be found at a location that is external to the electronic message (See Column 5, lines 11-19)

Referring to the rejection of claim 62, Maruyama et al. discloses wherein the credential includes biometric data (See Column 5,lines 13-14)

Referring to the rejection of claim 64, Maruyama et al. discloses wherein the electronic message is a HyperText Transport Protocol (HTTP) message, and wherein the header portion is a header portion of the HTTP message (See Column 8, lines 48-57)

Referring to the rejection of claims 65 and 68, Maruyama et al. discloses in a network environment that includes a plurality of computing systems capable of communicating using electronic messaging, a method for a recipient computing system to verify the identity of a sender of an electronic message, the method comprising the following:

an act of receiving the electronic message; (See Column 4, lines 10-22)

an act of reading an electronic signature from a header portion of the electronic message, the electronic signature generated by a user; (See Column 4, lines 23-29)

an act of reading a reference from the header portion, the reference indicating where a credential associated with the user may be found; (See Column 4, lines 23-29)

an act of using the reference to find the credential; and an act of determining if the credential corresponds with the electronic signature (See Column 6, lines 27-32)

Referring to the rejection of claim 66, Maruyama et al. discloses wherein the reference indicates that the associated credential may be found at a location that is internal to the electronic message (See Column 4, lines 23-29)

Referring to the rejection of claim 67, Maruyama et al. wherein the reference indicates that the associated credential may be found at a location that is external to the electronic message (See Column 4, lines 23-29)

Referring to the rejection of claim 69, Maruyama et al. wherein the one or more computer-readable media are physical storage media (See Column 4, lines 50-61)

Allowable Subject Matter

7. Claims 21,41,51,53, and 63 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

8. Claims 70-71 are allowed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cdf
September 14, 2007

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137